Stochastic o-minimal hybrid systems*

Thomas Brihaye, Mickael Randour, Cédric Rivière

Mathematics Department, Faculty of Science, UMONS – Université de Mons, Belgium

Abstract

Timed automata and *hybrid systems* are important frameworks for the analysis of continuous-time systems. In this ongoing work, we study a stochastic extension of the latter. There are clear challenges regarding decidability: (i) the reachability problem is already quickly undecidable for non-stochastic hybrid systems; (ii) even in the simpler setting of timed automata, the finite abstraction known as the region graph does not preserve its correctness when lifting it to the stochastic setting.

Our goal is to define the class of *stochastic o-minimal hybrid systems* (SoHSs) and to show that it ensures good properties while being reasonably rich (e.g., it encompasses continuous-time Markov chains). We look for *decisiveness* of SoHSs (as introduced by Adbulla et al.) and *definability* in our o-minimal structure. Hopefully, *approximation* of reachability probabilities could be obtainable in appropriate (and still quite rich) structures.

Hybrid systems and finite abstractions. *Timed automata* (TAs) [3, 4] and *hybrid systems* (HSs) [9, 2] are well-established formalisms for the modeling and analysis of timed systems. Roughly speaking, TAs are finite-state automata enriched with clocks and clock constraints. HSs can be seen as an extension of TAs where the clocks can be replaced by continuous variables with richer continuous behaviors. In both models, we distinguish between two kinds of transitions: *continuous transitions*, where the continuous variables evolve over time (e.g., according to a differential equation), and *discrete transitions*, where the system changes modes and variables can be reset.

A key result about TAs is the existence of a finite abstraction, known as the *region graph*, that induces a time-abstract bisimulation and thus is sufficient to verify many interesting properties on TAs. Among numerous important results deriving from the existence of the region graph, let us mention PSPACE-completeness of the reachability problem [3]. In parallel with such theoretical results, efficient verification tools have been implemented and successfully applied to industrial case studies [10, 14].

Unfortunately, the world of HSs is not as idyllic: we cannot guarantee the existence of a finite time-abstract bisimulation quotient [9], and the reachability problem is undecidable even for rather restricted classes of hybrid systems [11]. Obtaining classes of HSs with finite abstraction requires a fine balance between the discrete and continuous dynamics. The class of *initialized rectangular automata* [11] is such a compromise, where continuous variables follow independent trajectories within piecewise-linear envelopes and are reinitialized whenever the envelope changes. Another notable situation is the case of *o-minimal HSs* [13, 7], where the continuous dynamics is really rich, but the restriction on the discrete dynamics is severe: all continuous variables must be reset (non-deterministically, toward a given target set) after each discrete transition. For o-minimal HSs, the existence of a finite bisimulation quotient relies on two key ingredients: the strong reset assumption, and the nice finiteness properties induced by imposing on the continuous dynamics to be definable in an o-minimal structure [16] (see [8] for an overview on o-minimality).

Stochastic transition systems and decisiveness. In [1], Abdulla et al. introduced the elegant concept of *decisiveness* for denumerable Markov chains. Roughly speaking, decisiveness allows one to lift most good properties from finite Markov chains to denumerable ones, and therefore to adapt existing verification algorithms to infinite-state models.

*Work partially supported by F.R.S.-FNRS Incentive Grant for Scientific Research *ManySynth*; M. Randour is an F.R.S.-FNRS Research Associate.

When modeling complex (computer) systems, it is common to have interactions between real-time constraints and randomized aspects (see for instance [17]). Decisive Markov chains however do not encompass stochastic real-time systems. In [6], the concept of decisiveness was extended to general *stochastic transition systems* (STSs). As already mentioned, when considering models with dense time, a classical technique is to design a good abstraction that preserves some properties of the original model (such as the region graph for TAs). However, these abstractions generally do not preserve quantitative properties. For instance, when considering *stochastic timed automata* (STAs), the region graph — interpreted as a finite Markov chain — is not a correct abstraction to decide whether a state can be reached with probability one. In [6], a generic notion of abstraction is introduced, and decisiveness of the concrete model can be derived using similar properties on the abstraction.

Stochastic o-minimal hybrid systems. This abstract reports on an ongoing work whose goal is to instantiate the framework of [6] with a stochastic variant of o-minimal HSs. *Stochastic o-minimal hybrid systems* (SoHS) are o-minimal HSs extended with continuous probability distributions on both the time delays and the resets, and discrete distributions on the discrete transitions. Observe that *continuous-time Markov chains* can be seen as SoHSs with a single variable, always reset to zero, and exponential probability distributions.

We face two challenges to obtain interesting properties. The first one is to identify a minimal set of hypotheses which allow to fit the decisiveness framework of [6]. The second one concerns definability issues in o-minimal structures when introducing probability aspects.

Regarding the first challenge, we investigate an approach similar to the one used for single-clock STAs [6, Section 8.1.4]. More precisely, we intend to prove that the finite bisimulation on the underlying o-minimal HS (provided by [7]) is in fact a *sound α-abstraction* (in the sense of [6]). In order to prove the latter assumption, we need to identify a *finite attractor with good properties*: we aim to apply [6, Proposition 36]. As a by-product, we should conclude that SoHSs are decisive. Let us emphasize that this result is already of interest since STAs are not decisive in general. We could thus say that, in some sense, SoHSs are more robust to randomness compared to STAs (this is clearly due to the strong reset hypothesis).

Although already interesting, this first result might sound unsatisfying. Indeed, even if SoHSs are decisive, without a further effectiveness argument, we cannot apply any decision or approximation algorithm. The first step in this direction could be to provide a finite symbolic representation of the finite *sound α-abstraction*. In order to do so, the symbolic finite bisimulation provided by [7] is not sufficient since it gives no information on the probabilities to go from a symbolic state to another. The main difficulty here lies in the fact that *"a satisfactory theory of measure and integration seems to be lacking in the o-minimal context"* [5]. In particular, in an o-minimal structure, the primitive of a definable function is in general not definable in the same o-minimal structure. For instance, the function $\frac{1}{x}$ is definable in the ordered field of the real numbers, but its primitive $\ln|x|$ is not.

Regarding this second challenge, definability, we believe that the concepts of *(strongly) compatible* and *tame measures* on o-minimal structures [12] could serve our interests since they allow to consider o-minimal structures which are closed under integration with respect to a given measure (these structures are called *integrating o-minimal structures*).

Finally, decidability is not guaranteed in o-minimal structures. Let us mention the case of the ordered field of the real numbers expanded with the exponential function: decidability is open and linked to *Schanuel's conjecture*, a famous unsolved problem in transcendental number theory (see [15, 18]). Even definability is likely not sufficient to obtain decidability. Nevertheless, one could try to obtain an approximation scheme to compute reachability properties. This is not hopeless: for example, in the case of *probabilistic vector addition systems with states*, although one cannot decide whether the probability to reach a given upward-closed set is above a threshold, it is still possible to approximate such a probability [1]. In particular, we hope to obtain results for SoHSs definable in the o-minimal structure $\mathbb{R}_{an}$ — real numbers expanded with the restricted analytic functions (which is a an integrating o-minimal structure w.r.t. the Lebesgue measure [12]).

References

[1] Parosh A. Abdulla, Noomene Ben Henda, and Richard Mayr. Decisive Markov chains. *Logical Methods in Computer Science*, 3(4), 2007.

[2] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1):3–34, 1995.

[3] Rajeev Alur and David Dill. Automata for modeling real-time systems. In *ICALP'90: Automata, Languages, and Programming*, volume 443 of *Lecture Notes in Computer Science*, pages 322–335. Springer, 1990.

[4] Rajeev Alur and David Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[5] Alessandro Berarducci and Margarita Otero. An additive measure in o-minimal expansions of fields. *The Quarterly Journal of Mathematics*, 55(4):411–419, 2004.

[6] Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Pierre Carlier. When are stochastic transition systems tameable? *CoRR*, abs/1703.04806, 2017.

[7] Thomas Brihaye, Christian Michaux, Cédric Rivière, and Christophe Troestler. On o-minimal hybrid systems. In *HSCC'04: Hybrid Systems: Computation and Control*, volume 2993 of *Lecture Notes in Computer Science*, pages 219–233. Springer, 2004.

[8] Lou van den Dries. *Tame Topology and O-Minimal Structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1998.

[9] Thomas A. Henzinger. The theory of hybrid automata. In *LICS'96: Logic in Computer Science*, pages 278–292. IEEE Computer Society Press, 1996.

[10] Thomas A. Henzinger, Pei-Hsin Ho, and Howard Wong-Toi. A user guide to HyTech. In *TACAS'95: Tools and Algorithms for the Construction and Analysis of Systems*, volume 1019 of *Lecture Notes in Computer Science*, pages 41–71. Springer-Verlag, 1995.

[11] Thomas A. Henzinger, Peter W. Kopke, Anuj Puri, and Pravin Varaiya. What's decidable about hybrid automata. *Journal of Computer and System Sciences*, 57(1):94–124, 1998.

[12] Tobias Kaiser. First order tameness of measures. *Ann. Pure Appl. Logic*, 163(12):1903–1927, 2012.

[13] Gerardo Lafferriere, George J. Pappas, and Shankar Sastry. O-minimal hybrid systems. *Mathematics of Control, Signals, and Systems*, 13(1):1–21, 2000.

[14] Kim G. Larsen, Paul Pettersson, and Wang Yi. Uppaal: Status & developments. In *CAV'97: Computer Aided Verification*, volume 1254 of *Lecture Notes in Computer Science*, pages 456–459. Springer, 1997.

[15] Angus Macintyre and Alex J. Wilkie. On the decidability of the real exponential field. In *Kreiseliana*, pages 441–467. A K Peters, Wellesley, MA, 1996.

[16] Anand Pillay and Charles Steinhorn. Definable sets in ordered structures. I. *Transactions of the American Mathematical Society*, 295(2):565–592, 1986.

[17] Mariëlle Stoelinga. Fun with firewire: A comparative study of formal verification methods applied to the IEEE 1394 root contention protocol. *Formal Asp. Comput.*, 14(3):328–337, 2003.

[18] Alex J. Wilkie. Schanuel's conjecture and the decidability of the real exponential field. In *Algebraic model theory (Toronto, ON, 1996)*, volume 496 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 223–230. Kluwer Acad. Publ., Dordrecht, 1997.